

Symposium Gegevensmanagement

De AVG na mei 2018: waar staan we en hoe nu verder?

4 april 2019



Resumé: de belangrijkste verplichtingen



- Verantwoordingsplicht
- Verwerkingsregister
- Verwerkersovereenkomsten
- Passende technische- en organisatorische maatregelen
- Privacybeleid, reglementen en protocollen
- Privacy by Design en Privacy by Default
- Functionaris voor gegevensbescherming

Voorbeelden in de praktijk



**Heerhugowaardse huisarts mekkert:
'Nauwelijks toegang tot patiëntgegevens'**

**Zedendossier moordenaar
Anne Faber werd op zijn
verzoek niet gedeeld met
kliniek die hem behandelde**

Belastingdienst mag inkomensgegevens van huurders niet verstrekken
aan verhuurders

**Kwaliteit datalekregister bij
overheidsorganisaties loopt uiteen**

Knelpunten 'extern'

- AVG = risicogestuurde wetgeving met 'vage' normen
 - Vraagt om gedegen interpretatie
- Ontbreken grondslag voor verwerking (wet- en regelgeving)
 - Ontbreekt bijvoorbeeld aan bevoegdheden/taken
- Ontbreken normuitleg door Toezichthouder
 - Veel meldingen datalekken ≠ weinig (norm)uitleg
 - Veel klachten ≠ weinig (norm)uitleg

Knelpunten 'intern'

- Verwerkersrelatie en -overeenkomsten
- Inventarisatie voor verwerkingsregister verloopt moeizaam
- Aandacht voor AVG verslapt
- Window-dressing
- Draagvlak bij management en/of uitvoerende medewerkers
- Aanpak is ad hoc (risicogestuurd) en niet structureel
- Gegevensuitwisseling intern en met derden

Privacy Management



- Organisatorische maatregel als basis voor borging naleving AVG
- Een aantal belangrijke functies:
 - Privacy ambassadeurs/aanspreekpunten/accenthouders (1e lijns)
 - Privacy officer(s) (2e lijns)
 - FG (3e lijns)
 - Ciso
 - Informatie-/gegevensbeheerder
- Organisatie
 - Privacy (informatie) team
 - Bepaling en vastlegging rollen, taken, bevoegdheden en verantwoording
 - Structureel overleg en specifieke training privacy ambassadeurs

Onjuiste toepassing verwerkersrelatie

- Uitvoeren gegevensverwerking is niet de primaire taak?

Bijvoorbeeld:

- Banken
- Advocaten
- Telecomproviders
- Uitzend- of detacheringsbureau



Geen verwerkersrelatie

- Doel dienstverlening vs. doel gegevensverwerking

Beheer van het verwerkingsregister



- Het verwerkingsregister dient actueel en volledig te zijn
 - Geen momentopname
- Proces opstellen voor beheer en kwaliteitsmanagement verwerkingsregister
- Implementatie en borging nieuwe of gewijzigde systemen en processen in het verwerkingsregister
- Hiermee speelt het register een belangrijke rol in o.a :
 - Aantoonbaarheid en controleerbaarheid van compliance;
 - Als schakel tussen de business en privacy officer en FG.

Lessons learned



- **Inrichting Privacy Management**

- Samenstellen Privacy team en benoemen privacy ambassadeurs in lijn organisatie
- Bepalen, benoemen en beleggen van rollen, bevoegdheden, taken en verantwoording

- **(Her)beoordeel de (huidige) verwerkersrelaties en verwerkersovereenkomsten**

- Is er daadwerkelijk wel sprake van een verwerkersrelatie?
- Zorg voor duidelijke instructies voor inkopers/aanbesteding
- Extra aandacht afdwingbare maatregelen voor software, SAAS en web applicaties

- **Zorg voor borging van processen (aantoonbaarheid!):**

- Opstellen en inrichten (gezamenlijk 1^{ste} en 2^e lijns) proces en heartbeat voor beheer en kwaliteitsmanagement van het verwerkingsregister;
- AVG toevoegen aan proces pre-intakes en acceptatie systemen en processen;
- Documentatie (reglement/protocolen en praktische werk-instructies) voor processen vastleggen
- Awareness: onderwijs- en communicatieplan, o.a. documentatie/borging van trainingen/e-learning
- Het datalekkenregister voldoet aan de gestelde eisen (zie de [Handleiding van de AP](#))



www.privacycompany.eu
info@privacycompany.nl
070 – 820 96 90

Maanweg 174
Den Haag

